Introduction to number theory
Exercise sheet 1

`https://www.maths.tcd.ie/~mascotn/teaching/2020/MAU22301/index.html`

Version: October 5, 2020

Answers are due for Friday October 16th, 2PM.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Money money money (100 pts)*

How many ways are there to pay one million euros, using only 20 euro and 50 euro notes? (For instance, we could use 50,000 20 euro notes and 0 50 euro notes, or 25,000 20 euro notes and 10,000 50 euro notes, etc.)

Hint: Solve the Diophantine equation $20x + 50y = 1,000,000$.

NB you are not allowed to give a negative amount of one kind of notes, even to compensate for a large positive amounts of the other kind! So for instance, 100,000 20 euro notes plus -20,000 50 euro notes is not an acceptable form of payment — unless you claim to master the creation of antimatter, but I will definitely want to see proof of that.

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 2 *Euclid at work*

Prove that 2020 and 353 are coprime, and find integers u and v such that

$$2020u + 353v = 1.$$

Exercise 3 *An "obvious" factorisation*

1. Let $n \geq 2$ be an integer, and let $N = n^2 - 1$. Depending on the value of n, N can be prime or not; for example $N = 3$ is prime if $n = 2$, but $N = 8$ is composite if $n = 3$. Find all $n \geq 2$ such that N is prime.

   Hint: $a^2 - b^2 =$ *?*

2. Factor $N = 9999$ into primes. Make sure to prove that the factors you find are prime.

Exercise 4 *(In)variable gcd's*

Let $n \in \mathbb{Z}$.

1. Prove that $\gcd(n, 2n + 1) = 1$, no matter what the value of n is.

   Hint: How do you prove that two integers are coprime?

2. What can you say about $\gcd(n, n + 2)$?

Exercise 5 *Another algorithm for the gcd*

1. Let $a, b \in \mathbb{Z}$ be integers. Prove that $\gcd(a, b) = \gcd(b, a - b)$.

2. Use the previous question to design an algorithm to compute $\gcd(a, b)$ similar to the one seen in class, but using subtractions instead of Euclidean divisions. Demonstrate its use on the case $a = 50$, $b = 22$.

Exercise 6 *Product of coprimes*

Let a, b and c be integers. Suppose that a and b are coprime, and that a and c are coprime. Prove that a and bc are coprime.

Exercise 7 *Valuations*

1. Let $m = \prod_i p_i^{a_i}$, $n = \prod_i p_i^{b_i}$ be two integers, where the p_i are pairwise distinct primes. Prove that $m \mid n$ iff. $a_i \leqslant b_i$ for each i.

   Hint: If $n = km$, *consider the prime factorisation of* k.

2. In what follows, let $p \in \mathbb{N}$ be prime. Recall that for nonzero $n \in \mathbb{Z}$, we define $v_p(n)$ as the exponent of p in n. Prove that for all nonzero $n \in \mathbb{Z}$, $v_p(n)$ is the largest integer v such that $p^v \mid n$.

3. Recall that we set $v_p(0) = +\infty$ by convention. In view of the previous question, does this convention seem appropriate?

4. Let $m, n \in \mathbb{Z}$, both nonzero. Prove that $v_p(mn) = v_p(m) + v_p(n)$. What happens if m or n is zero?

5. Let $m, n \in \mathbb{Z}$, both nonzero. Prove that $v_p(m+n) \geqslant \min(v_p(m), v_p(n))$. What happens if m or n is zero?

6. Let $m, n \in \mathbb{Z}$. Prove that if $v_p(m) \neq v_p(n)$, then $v_p(m+n) = \min(v_p(m), v_p(n))$.

7. Give an example where $v_p(m+n) > \min(v_p(m), v_p(n))$.

Exercise 8 $\sqrt{n}$ *is either an integer or irrational*

Let n be a positive integer which is **not a square**, so that $\sqrt{n}$ is not an integer. The goal of this exercise is to prove that $\sqrt{n}$ is *irrational*, i.e. not of the form $\frac{a}{b}$ where a and b are integers.

1. Prove that there exists at least one prime p such that the p-adic valuation $v_p(n)$ is odd.

2. Suppose on the contrary that $\sqrt{n} = \frac{a}{b}$ with $a, b \in \mathbb{N}$; this may be rewritten as $a^2 = nb^2$. Examine the p-adic valuations of both sides of this equation, and derive a contradiction.

Exercise 9 *Divisors*

1. Factor 2020 into primes. Make sure to prove that you factorization is complete, i.e. that the factors you find are prime.

2. Deduce the number of divisors of 2020, and the sum of these divisors.

3. Do the same computations with 6000 instead of 2020.

Exercise 10 *Divisors again*

1. Find all integers $M \in \mathbb{N}$ of the form $3^a 5^b$ such that the sum of the positive divisors of M is 33883.

   Hint: $33883 = 31 \times 1093$*, and both factors are prime.*

2. Find all integers $L \in \mathbb{N}$ of the form $2^a 3^b$ such that the **product** of the divisors of L is 12^{15}.

   Hint: What are the divisors of L? Can you arrange them in a 2-dimensional array? Count the number of 2's, and deduce that the 2-adic valuation the product of all these divisors is $(b+1)(1+2+3+\cdots+a)$. What about the 3-adic valuation?

Exercise 11 *Fermat numbers*

Let $n \in \mathbb{N}$, and let $N = 2^n + 1$. Prove that if N is prime, then n must be a power of 2.

Hint: use the identity $x^m + 1 = (x+1)(x^{m-1} - x^{m-2} + \cdots - x + 1)$*, which is valid for all* ***odd*** $m \in \mathbb{N}$.

Remark: The Fermat numbers *are the* $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$. *They are named after the French mathematician Pierre de Fermat, who noticed that* F_0, F_1, F_2, F_3 *and* F_4 *are all prime, and conjectured in 1650 that* F_n *is prime for all* $n \in \mathbb{N}$. *However, this turned out to be wrong: in 1732, the Swiss mathematician Leonhard Euler proved that* $F_5 = 641 \times 6700417$ *is not prime. To this day, no other prime Fermat number has been found; in fact it is unknown if there is any ! This is because* F_n *grows very quickly with* n*, which makes it very difficult to test whether* F_n *is prime, even with modern computers.*

Exercise 12 *Perfect numbers*

A positive integer n is said to be *perfect* if it agrees with the sum of all of its divisors other than itself; in other words, if $\sigma_1(n) = 2n$. For instance, 6 is a perfect number, because its divisors other than itself are 1, 2 and 3, and $1 + 2 + 3 = 6$.

1. Let a be a positive integer, and let $n = 2^a(2^{a+1} - 1)$. Prove that if $2^{a+1} - 1$ is prime, then n is perfect.

   We now want to prove that all **even** perfect numbers are of this form.

2. Let n be an even number. Why may we find integers a and b such that $n = 2^a b$ and b is odd ?

3. In this question and in the following ones, we suppose that n is an even perfect number. Prove that $(2^{a+1} - 1) \mid b$.

4. Let thus $c \in \mathbb{N}$ be such that $b = (2^{a+1} - 1)c$. Prove that $\sigma_1(b) = b + c$.

5. Deduce that $c = 1$.

6. Conclude that $2^{a+1} - 1$ is prime.

7. Let $q \in \mathbb{N}$. Prove that if $2^q - 1$ is prime, then q is also prime.

   Hint: $x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1)$.

8. Find two even perfect numbers (apart from 6).

Remarks: Prime numbers of the form $2^q - 1$ *are called* Mersenne primes *after Marin Mersenne (French, 17th century). Not all numbers of the form* $2^q - 1$ *with* q *prime are prime, as the counter-example* $2^{11} - 1 = 23 \times 89$ *shows. In fact, as of today, only 49 primes* q *such that* $2^q - 1$ *is prime are known. As a result, only 49 Mersenne primes, and so only 49 even perfect numbers, are known. It is conjectured that there exist infinitely many Mersenne primes, and so infinitely many even perfect numbers, but this has never been proved. As for odd perfect numbers, if is unknown if any exist!*

Exercise 13 *Ideals of $\mathbb{Z}$*

In this exercise, we define an *ideal* of $\mathbb{Z}$ to be a subset $I \subseteq \mathbb{Z}$ such that

- I is not empty,
- whenever $i \in I$ and $j \in J$, we also have $i + j \in I$,
- whenever $x \in \mathbb{Z}$ and $i \in I$, we also have $xi \in I$.

1. Let $n \in \mathbb{Z}$. Prove that $n\mathbb{Z} = \{nx, \ x \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.
2. For which $m, n \in \mathbb{Z}$ do we have $m\mathbb{Z} = n\mathbb{Z}$?
3. Let $I \subset \mathbb{Z}$ be an ideal. Prove that whenever $i \in I$ and $j \in J$, we also have $-i \in I$, $i - j \in I$, and $0 \in I$.
4. Let $I \subset \mathbb{Z}$ be an ideal. Prove that there exists $n \in \mathbb{Z}$ such that $I = n\mathbb{Z}$.

   Hint: If $I \neq \{0\}$, let n be the smallest positive element of I, and consider the Euclidean division of the elements of i by n.
5. Prove that if I and J are ideals of $\mathbb{Z}$, then

   $$I + J = \{i + j \mid i \in I, j \in J\}$$

   is also an ideal of $\mathbb{Z}$.

   Hint: $i + j + i' + j' = i + i' + j + j'$.
6. Let now $a, b \in \mathbb{Z}$. By the previous question, $a\mathbb{Z} + b\mathbb{Z}$ is an ideal, so it is of the form $c\mathbb{Z}$ for some $c \in \mathbb{Z}$. Express c in terms of a and b.

   Hint: If you are lost, write an English sentence describing the set $a\mathbb{Z} + b\mathbb{Z}$.
7. Prove that if I and J are ideals of $\mathbb{Z}$, then so is their intersection $I \cap J$.
8. Let now $a, b \in \mathbb{Z}$. By the previous question, $a\mathbb{Z} \cap b\mathbb{Z}$ is an ideal, so it is of the form $c\mathbb{Z}$ for some $c \in \mathbb{Z}$. Express c in terms of a and b.